PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-269041**
(43)Date of publication of application : **20.09.2002**

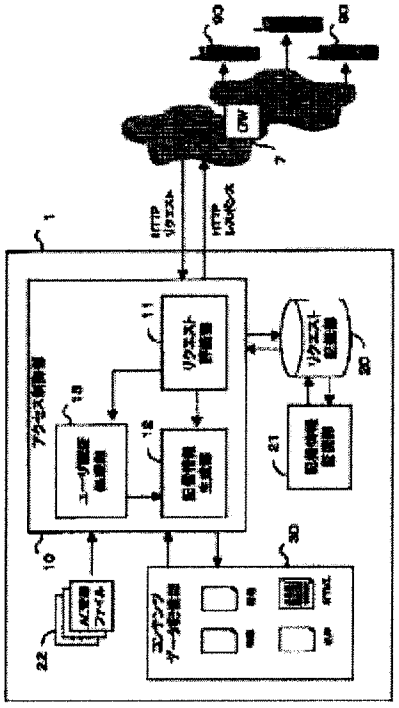
(51)Int.Cl. **G06F 15/00**
G06F 12/14
G06F 17/30
H04L 9/32

(21)Application number : **2001-066695**
(22)Date of filing : **09.03.2001**

(71)Applicant : **DAINIPPON PRINTING CO LTD**
(72)Inventor : **YAGI NOBUHIRO**
SUGIURA HIROAKI

(54) INFORMATION DISTRIBUTING SERVER DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information distributing server device which can authenticate a user without depending on terminal environment and can manage the valid period of authentication in information service on the Internet.
SOLUTION: The device is provided with a request recording part recording a request from an authenticated user, a recording information monitoring part which periodically inspects the record of the request recording part and deletes expired record and an access control part which urges user authentication information when the accessed user is not authenticated and authenticates the user by collating information with management information which is previously registered if the user is authenticated and returns a requested content with respect to the authenticated request. The users are authenticated for the respective contents and the authenticated user is requested to be authenticated again when prescribed time elapses. Consequently, the user is authenticated with high safety without depending on the environment of a terminal unit.



* NOTICES *

CLAIMS

[Claim(s)]

[Claim 1]The request Records Department which is a server system for performing a data communications service, and records a request from an attested user on a personal digital assistant, The recorded information Monitoring Department which deletes record which inspected record of the request Records Department periodically and passed the term of validity, As opposed to a user who a request from a user is received, and the user inspects whether you are those by whom user authentication was already done with reference to said request Records Department, and has not been attested yet, Press for user authentication information, receive user authentication information, compare with management information registered a priori, and user authentication is performed, Thus, an access control section which returns as a response contents data demanded by receiving without a request by which user authentication was carried out, or a request from a user by which user authentication had already been carried out, If a user who performed user authentication for every ******** and contents, and once did user authentication also does fixed time lapse, by user authentication being required again. Information distribution server equipment characterized by a feasible thing without depending on environment of a terminal equipment for user access control whose safety is higher than mere user authentication.

[Claim 2]The request Records Department which is a server system for performing a data communications service, and records a request from an attested user on a personal digital assistant, The recorded information Monitoring Department which deletes record which inspected record of the request Records Department periodically and passed the term of validity, A request evaluating part in which the user inspects whether you are those by whom user authentication was already done with reference to said request Records Department about a user who has accessed, A user authentication treating part which presses for user authentication information, receives user authentication information to a user who has not been attested yet, compares with management information registered a priori, and performs user authentication, A delivery information generation part which prepares or creates contents which should be distributed to a user, An access control section which receives ******** and a request from a user and returns suitable contents data as a response, If a user who performed user authentication for every ******** and contents, and once did user authentication also does fixed time lapse, by user authentication being required again. Information distribution server equipment characterized by a feasible thing without depending on environment of a terminal equipment for user access control whose safety is higher than mere user authentication.

[Claim 3]Request record of one affair recorded on said request Records Department, The information distribution server equipment according to claim 1 or 2 which is a thing containing information which identifies demanded contents at least, information which identifies a user who has accessed and time when the request record was recorded, or a term when the request record is effective.

[Claim 4]Information which identifies a user who is recorded on said request Records Department, and who has accessed, By using terminal identification information automatically added to request messages after acting as intermediary when a gateway unit which a cellular phone business operator installs relays request messages which a user sends, The information distribution server equipment according to claim 3 making it unnecessary for a user to perform a user-authentication-information input on a personal digital assistant while request record to the contents concerned of the user concerned is effective.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]In personal digital assistant-oriented the information distribution system or data communications service using the Internet, this invention relates to the mechanism of making only a specific user doing inspection permission of the contents.
[0002]
[Description of the Prior Art]As for the distribute information which used the Internet today, it is common to build WWW (World Wide Web) technology as a base. The text file with a tag as which WWW technology expresses contents (it is henceforth described as a contents file), It can be said that it is realized in HTTP (HyperText Transfer Protocal) which is a communications protocol between the WWW server which sends out a contents file etc., the WWW browser which interprets and displays a contents file, and a WWW server and a WWW browser. As a contents file form, HTML (HyperText Markup Language) is typical.
[0003]When a WWW server provides the contents data which is having access restriction specified in the information distribution system using the WWW technology for [general] a cellular phone, Usually, a WWW server acquires required ID and password from the client terminal which requires ID and a password of a requesting agency, and requires service in advance of sending of contents data. This procedure is realized using the structure called the basic authentication function with which a WWW server is provided as standard in many cases.
[0004]In basic authentication, if the contents which are having access restriction specified are requested, a WWW server will be returned to status code of ANOSORAIZUDO request-origin. Then, the requested WWW browser displays the interface which enters user ID and a password, and sends the inputted user authentication information to a WWW server. A WWW server performs user authentication for received ID and the password with reference to a password management file. As a result, if it is checked that it is access from a registered user, the demanded contents data will be sent to a requesting agency. Since a WWW browser memorizes the entered user ID and the password, Henceforth, unless a browser is terminated by a client side, when the page concerned is accessed again and user authentication information is required again, the memorized user ID and the password are automatically sent to a server by work of a WWW browser. Namely, once it succeeds in user authentication, unless a browser will be terminated, a contents inspection of the server concerned is unconditionally possible for a client side.
[0005]With the spread of cellular phones, the Internet was accessed from the cellular phone and the service which provides a mobile phone user with information has also begun from the site on the Internet. In order to provide such service, a cell phone service entrepreneur provides the Gateway which mediates between a portable telephone communication network and the Internet, performs required protocol conversion on this Gateway, and is making data exchange. However, since the browser which a cellular phone carries has various restrictions, it does not support the above-mentioned basic authentication in many cases.
[0006]
[Problem to be solved by the invention]There are two problems which are listed to below in the above-mentioned conventional technology. The first, I hear that user authentication using a basic authentication function cannot be performed to what is not supporting a basic authentication function like the browser of a cellular phone, and it is. Since the second point will not be again attested unless a browser is terminated if attestation is finished at the time of first time access, I hear that others' illegal use etc. have a problem also in respect of security, and it has them.
[0007]Let it be SUBJECT to provide the information distribution server equipment in which the attestation by which it is made in consideration of such a problem, and for which it does not depend on terminal environment is possible for this invention, and shelf-life management of attestation is

moreover possible.
[0008]
[Means for solving problem]In order to solve an aforementioned problem, the 1st mode of this invention, The request Records Department which is a server system for performing a data communications service, and records the request from an attested user on a personal digital assistant, The recorded information Monitoring Department which deletes the record which inspected record of the request Records Department periodically and passed the term of validity, As opposed to the user who the request from a user is received, and the user inspects whether you are those by whom user authentication was already done with reference to said request Records Department, and has not been attested yet, Press for user authentication information, receive user authentication information, compare with the management information registered a priori, and user authentication is performed, Thus, the access control section which returns as a response the contents data demanded by receiving without the request by which user authentication was carried out, or the request from a user by which user authentication had already been carried out, If the user who performed user authentication for every ******** and contents, and once did user authentication also does fixed time lapse, by user authentication being required again. It is information distribution server equipment characterized by a feasible thing without depending on the environment of a terminal equipment for the user access control whose safety is higher than mere user authentication.
[0009]When a person's request record by which user authentication was carried out is recorded on said request Records Department and said recorded information Monitoring Department deletes periodically the request record which passed the term of validity, Since user authentication will be again required if the user who once did user authentication also does fixed time lapse, it becomes possible to perform user access control whose safety is higher than mere user authentication. The request from a user by which user authentication is not carried out is received, Since it presses for user authentication information by work of an access control section by the server side and user authentication information is received, even when the personal digital assistant side does not support the basic authentication function of a WWW server, user authentication can be carried out without being dependent on the environment of a user's terminal equipment. * NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is an entire configuration figure of the information distribution server equipment 1.
[Drawing 2]It is a flow chart explaining operation of the access control section 10.
[Drawing 3]It is an operation flow figure of the recorded information Monitoring Department 21.
[Drawing 4]It is a figure showing the example of the request information recorded on the request Records Department 20.
[Explanations of letters or numerals]
1 Information distribution server equipment
7 Gateway
8 Portable telephone communication network
9 Internet
10 Access control section
11 Request evaluating part

12 Delivery information generation part
13 User authentication treating part
20 Request Records Department
21 Recorded information Monitoring Department
22 Access control file
30 Contents data storage part
90 Personal digital assistant

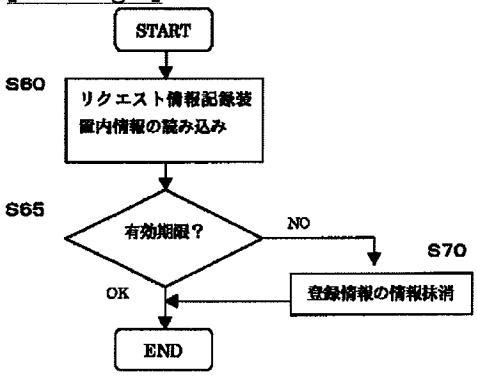
[Translation done.]

* NOTICES *

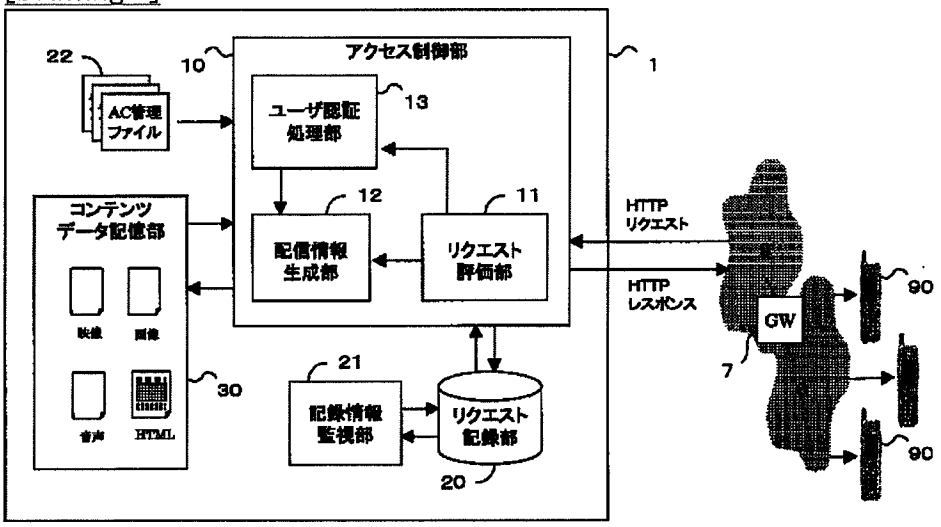
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

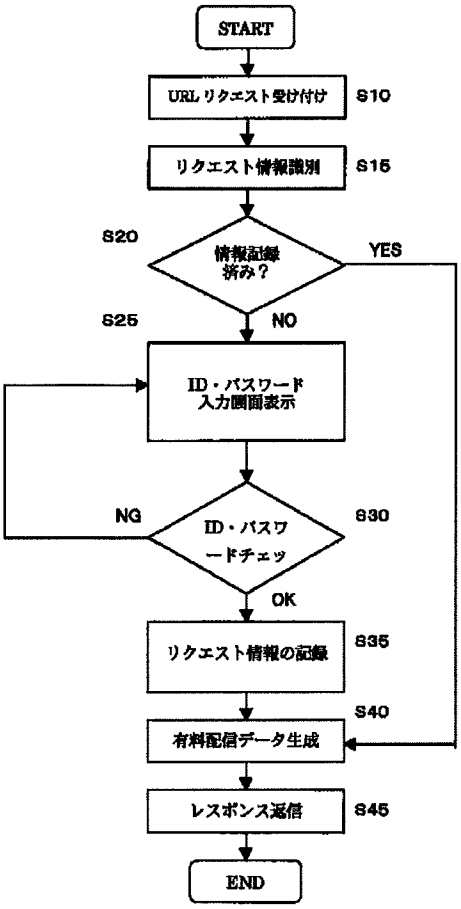
[Drawing 3]



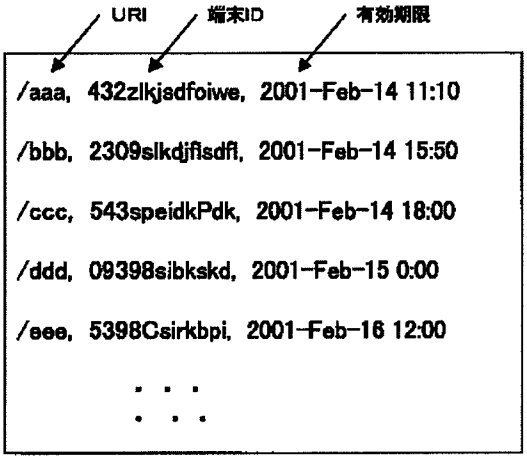
[Drawing 1]



[Drawing 2]



[Drawing 4]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－269041
（P2002－269041A）
(43)公開日　平成14年９月20日(2002.9.20)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｂ	５Ｂ０１７
	12/14	３２０	12/14	３２０Ｆ	５Ｂ０７５
	17/30	１１０	17/30	１１０Ｆ	５Ｂ０８５
				１１０Ｇ	５Ｊ１０４
		１２０		１２０Ｂ	

審査請求　未請求　請求項の数４　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願2001－66695(P2001－66695)

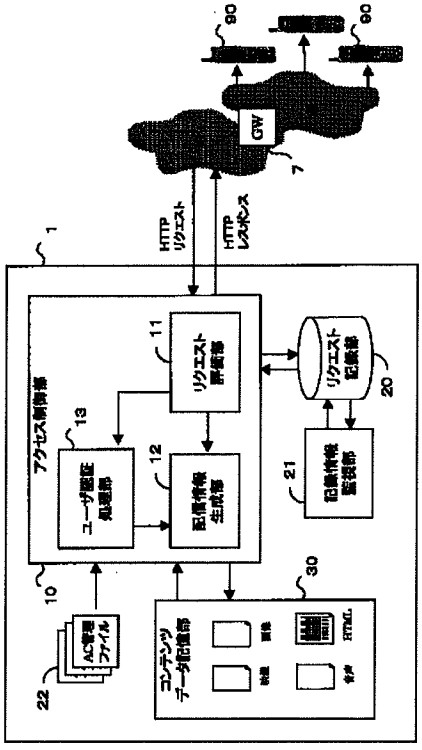
(22)出願日　平成13年３月９日(2001.3.9)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　八木　伸公
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　杉浦　博昭
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　100111659
弁理士　金山　聡

最終頁に続く

(54)【発明の名称】　情報配信サーバー装置

(57)【要約】
【課題】インターネット上の情報サービスにおいて、端末環境に依存しないユーザ認証が可能で、しかも認証の有効期間管理が可能な情報配信サーバー装置を提供することを課題とする。
【解決手段】認証済みユーザからのリクエストを記録するリクエスト記録部と、リクエスト記録部の記録を定期的に検査し有効期限を過ぎた記録を削除する記録情報監視部と、アクセスしてきた利用者が未認証ユーザであれば、ユーザ認証情報を催促し、そうでなければ事前に登録してある管理情報と照合してユーザ認証を行い、このように認証されたリクエストに対して要求されたコンテンツを返信するアクセス制御部と、を備えて、コンテンツ毎にユーザ認証を行い、かつ一旦ユーザ認証した利用者も一定時間経過すると、再びユーザ認証を要求されることで、安全性の高いユーザ認証を端末機器の環境に依存せずに実施可能な情報配信サーバー装置により上記課題を解決する。



1

【特許請求の範囲】

【請求項１】　携帯端末に情報配信サービスを行うためのサーバー装置であって、認証済みユーザからのリクエストを記録するリクエスト記録部と、リクエスト記録部の記録を定期的に検査し有効期限を経過した記録を削除する記録情報監視部と、利用者からのリクエストを受付けて、前記リクエスト記録部を参照して、その利用者が既にユーザ認証された者であるかを検査し、まだ認証されていない利用者に対しては、ユーザ認証情報を催促し、ユーザ認証情報を受付け、事前に登録してある管理情報と照合してユーザ認証を行い、このようにユーザ認証されたリクエスト、または既にユーザ認証されていたユーザからのリクエスト、に対して要求されたコンテンツデータをレスポンスとして返すアクセス制御部と、を備えて、コンテンツ毎にユーザ認証を行い、かつ一旦ユーザ認証した利用者も一定時間経過すると、再びユーザ認証を要求されることで、単なるユーザ認証よりも安全性の高いユーザアクセス制御を端末機器の環境に依存せずに実施可能なことを特徴とする情報配信サーバー装置。

【請求項２】　携帯端末に情報配信サービスを行うためのサーバー装置であって、認証済みユーザからのリクエストを記録するリクエスト記録部と、リクエスト記録部の記録を定期的に検査し有効期限を経過した記録を削除する記録情報監視部と、アクセスしてきた利用者について、その利用者が既にユーザ認証された者であるかを前記リクエスト記録部を参照して検査するリクエスト評価部と、まだ認証されていない利用者に対しては、ユーザ認証情報を催促し、ユーザ認証情報を受付け、事前に登録してある管理情報と照合してユーザ認証を行うユーザ認証処理部と、利用者に配信すべきコンテンツを準備または作成する配信情報生成部と、を備えて、利用者からのリクエストを受付けて適切なコンテンツデータをレスポンスとして返すアクセス制御部と、を備えて、コンテンツ毎にユーザ認証を行い、かつ一旦ユーザ認証した利用者も一定時間経過すると、再びユーザ認証を要求されることで、単なるユーザ認証よりも安全性の高いユーザアクセス制御を端末機器の環境に依存せずに実施可能なことを特徴とする情報配信サーバー装置。

【請求項３】　前記リクエスト記録部に記録される１件のリクエスト記録は、少なくとも、要求したコンテンツを識別する情報、アクセスしてきた利用者を識別する情報、および、そのリクエスト記録が記録された時刻またはそのリクエスト記録が有効な期限、を含むものである請求項１または請求項２に記載の情報配信サーバー装置。

【請求項４】　前記リクエスト記録部に記録されるアクセスしてきた利用者を識別する情報は、携帯電話事業者の設置するゲートウエイ装置が、利用者の発信するリクエストメッセージを中継する時に中継後のリクエストメッセージに自動的に付加する端末識別情報を利用することにより、当該利用者の当該コンテンツへのリクエスト記録が有効な間は、利用者が携帯端末上でユーザ認証情報入力を行うことを不要としたことを特徴とする請求項３に記載の情報配信サーバー装置。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットを利用した携帯端末向けの情報配信システムあるいは情報配信サービスにおいて、コンテンツを特定の利用者だけに閲覧許可させる仕組みに関する。

【０００２】

【従来技術】今日インターネットを利用した情報配信はWWW（World Wide Web）技術をベースとして構築することが普通である。WWW技術は、コンテンツを表現するタグ付きのテキストファイル（以後コンテンツファイルと記す）、コンテンツファイル等を送り出すWWWサーバー、コンテンツファイルを解釈し表示するWWWブラウザ、WWWサーバーとWWWブラウザ間の通信プロトコルであるＨＴＴＰ（HyperText Transfer Protocal）で成り立つといえる。コンテンツファイル形式としてはＨＴＭＬ（HyperText Markup Language）が代表的である。

【０００３】一般の、携帯電話を対象としないWWW技術を用いた情報配信システムにおいて、WWWサーバーがアクセス制限を指定されているコンテンツデータを提供する場合は、通常WWWサーバーは、コンテンツデータの送付に先立ち、ＩＤ・パスワードをリクエスト元に要求し、サービスを要求するクライアント端末から必要なＩＤ・パスワードを取得する。この手続きは、WWWサーバーが標準で備えるベーシック認証機能と呼ばれる仕組みを用いて実現されることが多い。

【０００４】ベーシック認証では、アクセス制限を指定されているコンテンツがリクエストされるとWWWサーバーはアンオーソライズドのステイタスコードをリクエスト元に返す。するとリクエストしたWWWブラウザはユーザＩＤ･パスワードを入力するインターフェースを表示し、入力されたユーザ認証情報をWWWサーバーに送る。WWWサーバーは受け取ったＩＤ・パスワードをパスワード管理ファイルを参照してユーザー認証を行う。この結果、登録済みユーザーからのアクセスであることが確認されれば、要求されたコンテンツデータをリクエスト元に送付する。WWWブラウザは入力されたユーザＩＤ･パスワードを記憶するので、以後、クライアント側でブラウザを終了させない限り、当該ページに再びアクセスして再度ユーザ認証情報を要求された時は、記憶していたユーザＩＤ･パスワードをWWWブラウザの働きにより自動的にサーバーに送付する。すなわち、一度ユーザ認証に成功すれば、ブラウザを終了させない限り、クライアント側は無条件に当該サーバーのコンテン

ツ閲覧が可能である。

【０００５】携帯電話の普及に伴い、携帯電話からインターネットに接続して、インターネット上のサイトから携帯電話利用者に情報を提供するサービスも始まっている。このようなサービスを提供するために携帯電話サービス事業者は、携帯電話通信網とインターネットを橋渡しするゲートウエイを設けて、このゲートウエイの上で必要なプロトコル変換を行ってデータのやり取りを行なわせている。しかしながら、携帯電話が搭載するブラウザは、様々な制約があるため上記ベーシック認証には対応していないことが多い。

【０００６】

【発明が解決しようとする課題】上記の従来技術では以下に挙げるような二つの問題がある。その第一は、携帯電話のブラウザのようなベーシック認証機能をサポートしていないものに対しては、ベーシック認証機能を利用したユーザー認証を行えないということである。また、第二点は、初回アクセス時に認証を済ませると、ブラウザを終了させない限り再び認証されないので他人の不正利用などセキュリティー面でも問題があるということである。

【０００７】本発明はこのような問題点を考慮してなされたものであり、端末環境に依存しない認証が可能で、しかも認証の有効期間管理が可能な情報配信サーバー装置を提供することを課題とする。

【０００８】

【課題を解決するための手段】上記課題を解決するため、本発明の第１の態様は、携帯端末に情報配信サービスを行うためのサーバー装置であって、認証済みユーザからのリクエストを記録するリクエスト記録部と、リクエスト記録部の記録を定期的に検査し有効期限を経過した記録を削除する記録情報監視部と、利用者からのリクエストを受付けて、前記リクエスト記録部を参照して、その利用者が既にユーザ認証された者であるかを検査し、まだ認証されていない利用者に対しては、ユーザ認証情報を催促し、ユーザ認証情報を受付け、事前に登録してある管理情報と照合してユーザ認証を行い、このようにユーザ認証されたリクエスト、または既にユーザ認証されていたユーザからのリクエスト、に対して要求されたコンテンツデータをレスポンスとして返すアクセス制御部と、を備えて、コンテンツ毎にユーザ認証を行い、かつ一旦ユーザ認証した利用者も一定時間経過すると、再びユーザ認証を要求されることで、単なるユーザ認証よりも安全性の高いユーザアクセス制御を端末機器の環境に依存せずに実施可能なことを特徴とする情報配信サーバー装置である。

【０００９】前記リクエスト記録部に、ユーザ認証された者のリクエスト記録を記録し、前記記録情報監視部が有効期限を経過したリクエスト記録を定期的に削除することにより、一旦ユーザ認証した利用者も一定時間経過すると、再びユーザ認証を要求されるので、単なるユーザ認証よりも安全性の高いユーザアクセス制御を行うことが可能となる。また、ユーザ認証されていない利用者からのリクエストに対しては、サーバー側でアクセス制御部の働きによりユーザ認証情報を催促し、ユーザ認証情報を受付けるので、携帯端末側がWWWサーバーのベーシック認証機能に対応していない場合でも、利用者の端末機器の環境に依存せずにユーザ認証を実施することができる。

【００１０】また、上記課題を解決するための、本発明のより具体的な第２の態様は、携帯端末に情報配信サービスを行うためのサーバー装置であって、認証済みユーザからのリクエストを記録するリクエスト記録部と、リクエスト記録部の記録を定期的に検査し有効期限を経過した記録を削除する記録情報監視部と、アクセスしてきた利用者について、その利用者が既にユーザ認証された者であるかを前記リクエスト記録部を参照して検査するリクエスト評価部と、まだ認証されていない利用者に対しては、ユーザ認証情報を催促し、ユーザ認証情報を受付け、事前に登録してある管理情報と照合してユーザ認証を行うユーザ認証処理部と、利用者に配信すべきコンテンツを準備または作成する配信情報生成部と、を備えて、利用者からのリクエストを受付けて適切なコンテンツデータをレスポンスとして返すアクセス制御部と、を備えて、コンテンツ毎にユーザ認証を行い、かつ一旦ユーザ認証した利用者も一定時間経過すると、再びユーザ認証を要求されることで、単なるユーザ認証よりも安全性の高いユーザ認証を端末機器の環境に依存せずに実施可能なことを特徴とする情報配信サーバー装置である。

【００１１】本発明のさらに好ましい第３の態様としては、前記第１または第２の態様の情報配信サーバー装置において、前記リクエスト記録部に記録される１件のリクエスト記録は、少なくとも、要求したコンテンツを識別する情報、アクセスしてきた利用者を識別する情報、および、そのリクエスト記録が記録された時刻またはそのリクエスト記録が有効な期限、を含むものである。

【００１２】さらに好ましい態様としては、前記第３の態様の情報配信サーバー装置において、前記リクエスト記録部に記録されるアクセスしてきた利用者を識別する情報は、携帯電話事業者の設置するゲートウエイ装置が、利用者の発信するリクエストメッセージを中継する時に中継後のリクエストメッセージに自動的に付加する端末識別情報を利用することにより、当該利用者の当該コンテンツへのリクエスト記録が有効な間は、利用者が携帯端末上でユーザ認証情報入力を行うことを不要としたものである。

【００１３】ここで、端末識別情報は携帯電話事業者が一定の条件で希望する利用者の携帯端末に与えるものである。従来のWWW技術におけるベーシック認証手段においては、一旦ユーザ認証を行った後は、WWWブラウ

ザがユーザＩＤ･パスワードを記憶し、以後のアクセスでは、WWWブラウザが自動的に記憶しているユーザＩＤをリクエストメッセージに付加するため、利用者は何度もユーザ認証情報を入力する必要がなかった。ところが、本発明の情報配信サーバー装置では、利用者端末側でそのような機能を前提としないため、一旦ユーザ認証した後の同一利用者からの再アクセスに対してどのように利用者を識別するかの問題点があった。そのリクエスト記録が有効な間であっても、アクセスする度にユーザ認証入力を行うのでは不便である。しかしこの問題は、上記のように、携帯電話事業者の設置するゲートウエイ装置が、利用者の発信するリクエストメッセージを中継する時に中継後のリクエストメッセージに自動的に付加する端末識別情報を利用することで解決した。

【００１４】

【発明の実施の形態】以下、図面を用いて、本発明の好適な実施形態である情報配信サーバー装置１を説明してゆく。図１は、情報配信サーバー装置１（以下サーバー装置１）の全体構成図である。サーバー装置１は、アクセス制御部１０、リクエスト記録部２０、記録情報監視部２１、コンテンツ毎にアクセス可能なユーザを記録したアクセス管理ファイル２２、および、コンテンツデータ記憶部３０から構成される。サーバー装置１は、インターネット９と、インターネット９と携帯電話通信網８とを接続するゲートウエイ７を通じて、利用者の使用する携帯端末９０とコンテンツデータおよびメッセージのやり取りを行う。サーバー装置１と携帯電話事業者が設置するゲートウエイ７は、ＨＴＴＰ（HyperText Transfer Protocol）によりリクエストとレスポンスのメッセージをやり取りする。尚、以下の記載ではＨＴＴＰによるリクエストメッセージおよびレスポンスメッセージを、それぞれＨＴＴＰリクエスト、ＨＴＴＰレスポンスと略記する。

【００１５】携帯端末９０は、コンテンツファイルを解釈して表示するラウザを搭載した携帯電話等であって、サーバー装置１に対してクライアント端末として機能する。携帯端末９０は各々固有の端末識別情報を有することを前提とする。端末識別情報は携帯電話事業者が一定の条件で希望する利用者の携帯端末に与えるものである。携帯端末９０は携帯通信モジュールを接続したパソコンやＰＤＡ等の携帯端末でもよい。

【００１６】アクセス制御部１０は、ユーザからのリクエストメッセージを受け付け、幾つかの必要な処理を実行し、最終的にリクエストに応じた結果を応答メッセージにしてユーザに返すよう働く。アクセス制御部１０には、リクエスト評価部１１、配信情報生成部１２、ユーザ認証処理部１３が内蔵されている。アクセス制御部１０は、具体的には、ＨＴＴＰリクエストを受け付け、リクエストに応じた結果を応答メッセージにしてユーザに返すWWWサーバソフトウエアとこのWWWサーバから呼出される幾つかのソフトウエアプログラムで実現できる。

【００１７】リクエスト評価部１１は、アクセス制御部１０が受付けたＨＴＴＰリクエストのリクエストＵＲＩ（Uniform Resource Identifier）と端末ＩＤが、後述するリクエスト記録部２０に記録されているかどうかの判定を行う。ＵＲＩはコンテンツを指定する識別情報である。リクエスト記録部２０の情報は参照のみ行う。

【００１８】リクエスト記録部２０は、ユーザー認証後のリクエスト情報、すなわちリクエストＵＲＩと端末ＩＤが、その有効期限とともに記録される。

【００１９】ユーザー認証処理部１３は、リクエスト評価部１１の判定の結果、リクエスト情報が記録されていなかった時に起動され、受付けたリクエストに対してユーザー認証行う。すなわち、ユーザＩＤ･パスワードを要求する対話インターフェースを生成するデータをリクエスト元に送出し、アクセスしてきた利用者に、設定されているユーザＩＤ・パスワードの入力を促す。そして返答結果を受取りコンテンツ毎に用意されているアクセス管理ファイル２２を参照して、入力されたユーザＩＤ･パスワードが当該コンテンツのアクセス管理ファイル２２に設定されているかどうか検査する。アクセス管理ファイル２２内に一致するユーザＩＤ･パスワードがあれば、認証がなされたことになる。ユーザ認証処理部１３は、現在時刻にアクセス管理ファイル２２に記載されている当該コンテンツの認証後有効時間を加えた時刻を有効期限の時刻として算出し、リクエストされたＵＲＩと当該ユーザの端末ＩＤとこの有効期限をリクエスト情報としてリクエスト記録部２０に記録する。そして、配信情報生成部１２に処理を促す。図４にリクエスト情報の記録内容例を示す。

【００２０】配信情報生成部１２は、指定されたＵＲＩに従って表示するコンテンツを生成する。実際には、コンテンツを生成するプログラム、または、様々な素材データとのリンクを含むコンテンツファイルである。

【００２１】記録情報監視部２１は、リクエスト情報の時間管理を行う。登録されているリクエスト情報が有効期間を超えている場合はその情報を抹消する。

【００２２】コンテンツデータ記憶部３０は、配信用のコンテンツファイル及び素材データを記録格納するハードディスク等のメモリである。

【００２３】図２はサーバー装置１の主要部であるアクセス制御部１０の処理の流れを示すフロー図である。図２に従って、サーバー装置１が利用者からのコンテンツリクエストメッセージを受けてからコンテンツデータをレスポンスとして返すまでの処理フローを説明する。

【００２４】アクセス制御部１０はＨＴＴＰリクエストを受け取ると、リクエストＵＲＩと端末ＩＤをリクエスト情報として抽出し（Ｓ１０）、リクエスト評価部１１を呼出す。リクエスト評価部１１は、抽出したリクエス

ト情報がリクエスト情報記録部２に記録済みかどうか検査する（Ｓ１５）。記録済みの場合、ユーザー認証処理は行わずに配信情報生成部１２に処理を促す（Ｓ４０）。未記録の場合はユーザ認証処理部１３に処理を促す。

【００２５】ユーザ認証処理部１３は、クライアント端末にＩＤ・パスワード入力ウインドウを表示させるデータを送出し、アクセスしてきた利用者にＩＤ・パスワードの入力を促す（Ｓ２５）。利用者によって入力されたＩＤ・パスワードとコンテンツ毎に設定されているアクセス管理ファイル２２に記録されているＩＤ・パスワードを照合し（Ｓ３０）、一致していたらリクエスト情報記録部２０に、現在時刻とリクエスト情報を記録し（Ｓ３５）、配信情報生成部１２に処理を促す（Ｓ４０）。一致していなかったらステップＳ２５に戻る。

【００２６】配信情報生成部１２で、生成または既存のファイルを読み出すことにより準備されたデータはＨＴＴＰレスポンスを構成してリクエスト元のクライアント端末へ返信される（Ｓ４５）。以上がリクエストメッセージを受付けてから応答を返すまでのアクセス制御部１０の動作である。

【００２７】リクエストＵＲＩとＨＴＴＰリクエストに付加される端末ＩＤがリクエスト記録部２０にリクエスト情報として記録される。リクエスト情報の有効期間はサービス毎にまたはコンテンツ毎に設定されている。有効期間を越えた場合、リクエスト情報記録装置の記録内容は全て無効となる（削除される）。有効期間を越えてリクエストを受け取った場合は、リクエスト元に対して初回アクセスとしてユーザー認証情報を要求する。

【００２８】次に記録情報監視部２１の働きを述べる。図３は、記録情報監視部２１の動作フロー図である。記録情報監視部２１は定期的にリクエスト記録部を参照し、有効期限を超過したリクエスト情報があるかどうか検査する（Ｓ６０）。有効期限を超過したリクエスト記録を見つけた場合は、そのリクエスト記録を抹消する（Ｓ７０）。

＊【００２９】以上、利用者へのアクセス制限手段に特徴がある情報配信サーバー装置１を詳しく説明した。

【００３０】

【発明の効果】本発明による情報配信サーバー装置によれば、クライアント側でベーシック認証機能をサポートしていない場合でも、ベーシック認証と同等の機能を提供することが可能となるため、携帯端末をクライアントとして用いる情報配信システムを構築する際、または携帯端末向けの情報配信サービスを提供する際、携帯端末の仕様の違いを考慮する必要がなく大変便利である。また、ベーシック認証と比べると、コンテンツの有効期限管理が行える為、期間限定の配信サービスが可能となるという顕著な効果を奏することができる。

【図面の簡単な説明】

【図１】　情報配信サーバー装置１の全体構成図である。

【図２】　アクセス制御部１０の動作を説明するフローチャートである。

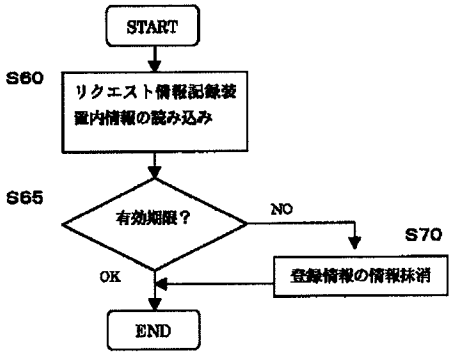
【図３】　記録情報監視部２１の動作フロー図である。

【図４】　リクエスト記録部２０に記録されるリクエスト情報の例を示す図である。

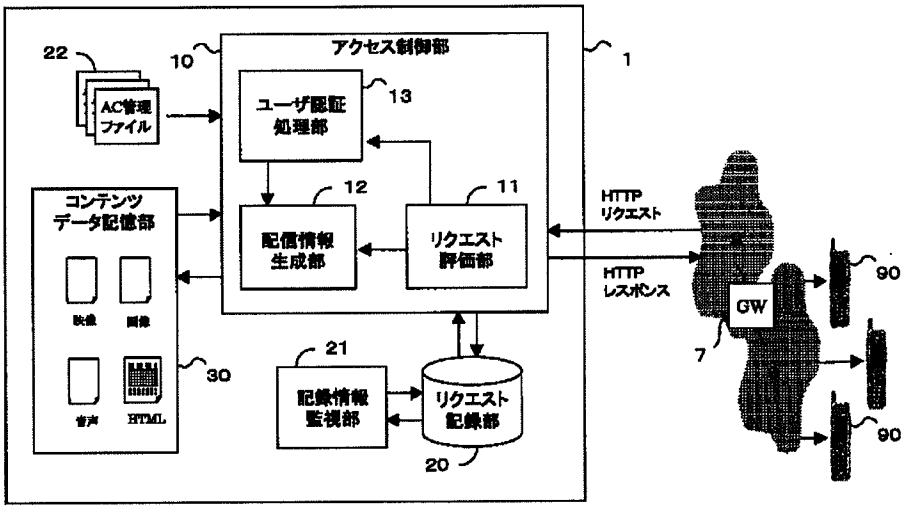
【符号の説明】

１	情報配信サーバー装置
７	ゲートウエイ
８	携帯電話通信網
９	インターネット
１０	アクセス制御部
１１	リクエスト評価部
１２	配信情報生成部
１３	ユーザ認証処理部
２０	リクエスト記録部
２１	記録情報監視部
２２	アクセス管理ファイル
３０	コンテンツデータ記憶部
９０	携帯端末

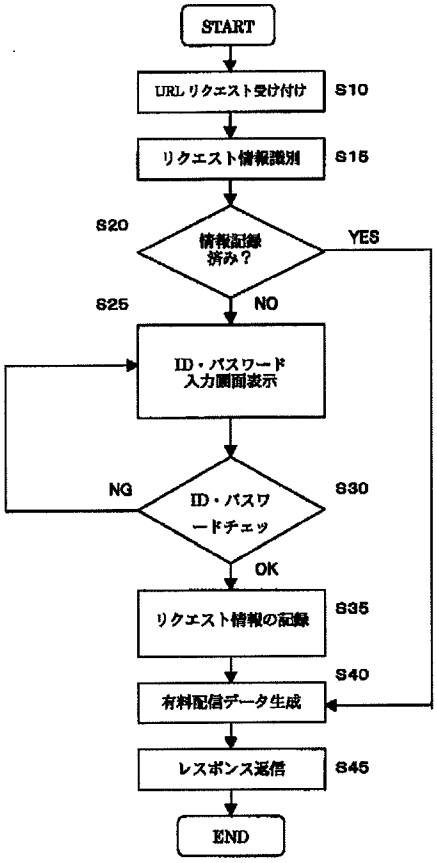
【図３】



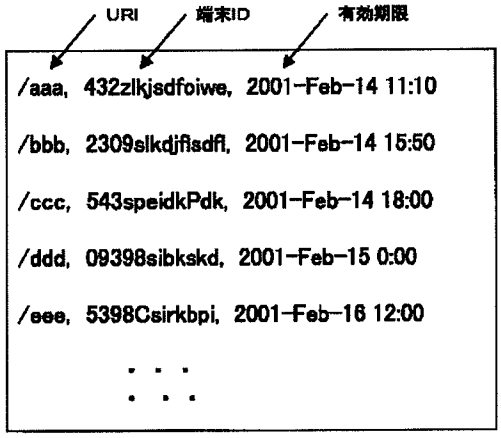
【図１】


22
10
アクセス制御部
1
AC管理ファイル
ユーザ認証処理部
13
12
11
コンテンツデータ記憶部
配信情報生成部
リクエスト評価部
HTTP リクエスト
HTTP レスポンス
GW
90
7
90
30
21
記録情報監視部
リクエスト記録部
20
映像
画像
音声
HTML

【図２】


START
URLリクエスト受け付け
S10
リクエスト情報識別
S15
S20
情報記録済み？
YES
NO
S25
ID・パスワード入力画面表示
NG
ID・パスワードチェッ
S30
OK
リクエスト情報の記録
S35
S40
有料配信データ生成
レスポンス返信
S45
END

【図４】


URI
端末ID
有効期限
/aaa, 432zlkjsdfoiwe, 2001-Feb-14 11:10
/bbb, 2309slkdjflsdfl, 2001-Feb-14 15:50
/ccc, 543speidkPdk, 2001-Feb-14 18:00
/ddd, 09398sibkskd, 2001-Feb-15 0:00
/eee, 5398Csirkbpi, 2001-Feb-16 12:00

フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ 9/32		Ｈ０４Ｌ 9/00	６７３Ａ	

Ｆターム(参考) 5B017 AA06 BA05 BB09 BB10 CA16
5B075 KK43 KK54 KK63 PQ05 PR03
5B085 AA08 AE02 AE03 BA06 BC01
5J104 AA07 KA01 NA05 PA02